AUDET & PARTNERS, LLP
MARK BURTON (SBN 154061)
Email: mburton@audetlaw.com
MICHAEL MCSHANE (SBN 127944)
Email: mmcshane@audetlaw.com
LING Y. KUANG (SBN 296873)
Email: lkuang@audetlaw.com
711 Van Ness Ave., Suite 500
San Francisco, CA 94102
(415) 568-2555 Telephone
(415) 568-2556 Facsimile

ZIMMERMAN REED LLP
CALEB MARKER (SBN 269721)
Email: caleb.marker@zimmreed.com
2381 Rosecrans Ave., Suite 328
Manhattan Beach, CA 90245
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

Attorneys for Plaintiff and for the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL GONZALES, individually, and on behalf of himself and all others similarly situated,

Plaintiff,

v.

UBER TECHNOLOGIES, INC., a Delaware corporation; UBER USA, LLC, a Delaware limited liability company; RAISER-CA. LLC, a Delaware limited liability company; and, DOES 1 to 10, inclusive,

Defendants.

Case No. 3:17-cv-02264-JSC

Assigned for all purposes to the Honorable Jacqueline Scott Corley

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED CLASS ACTION COMPLAINT

Hearing Date: September 20, 2018
Time: 9:00 a.m.
Courtroom: F-15th Floor

Date Action Filed: April 24, 2017

TABLE OF CONTENTS

INTRODUCTION **1**

ARGUMENT **2**

I. Plaintiff Asserts Valid Claims for Violations of the Unfair Competition Law. 2

A. Plaintiff has Stated a Claim for Injunctive Relief 3

B. Plaintiff has Stated a Claim for Restitution 6

II. Plaintiff Asserts a Valid Claim for Violations of the Stored Communication Act. 7

A. Plaintiff has Alleged That the Data Defendants' Accessed Were Stored for Purposes of Backup Protection 7

B. Plaintiff has Adequately Alleged Lyft's Servers Qualify as "a facility through which an electronic communication services is provided" 10

III. Plaintiff Asserts a Valid Claim for Violations of the CDAFA. 10

A. Plaintiff Owns the Data at Issue 10

B. Defendants Accessed the Data Without Permission 12

C. Plaintiff Has Sustained Damages as a Result of Defendant's Conduct 13

IV. Plaintiff Asserts a Valid Claim for Constitutional Invasion of Privacy 14

A. Plaintiff Alleges Invasion of a Legally Protected Privacy Interest 15

B. Plaintiff Maintained a Reasonable Expectation of Privacy in his SGD 16

C. Defendants' Conduct Amounts to a Serious Invasion of Plaintiff's Privacy Interests 18

D. Defendants Have No Legitimate Justification for their Invasion 19

CONCLUSION **20**

TABLE OF AUTHORITIES

Page(s)

Cases

Aguilar v. Avis Rent A Car System, Inc.,
21 Cal.4th 121 (Cal. 1999) 6

Am. Acad. of Pediatrics v. Lungren,
16 Cal. 4th 307 (Cal. 1997) 16

U.S. v. Jones,
565 U.S. 4001 (2012) 15

Backhaut v. Apple, Inc.,
74 F. Supp. 3d 1033 (N.D. Cal. 2014) 10

Barquis v. Merchants Collection Ass'n of Oakland, Inc.,
7 Cal.3d 94 (Cal. 1972) 3

Broughton v. Cigna Healthplans,
21 Cal.4th 1066 (Cal. 1999) 3, 4

Capitol Audio Access, Inc. v. Umemoto,
980 F. Supp. 2d 1154 (E.D. Cal. 2013) 14

Carpenter v. United States,
138 S. Ct. 2206 (2018) ..... *passim*

Cline v. Reetz-Laiolo,
Nos. 3:17-cv-06866, 3:17-cv-06867, 2018 WL 3159248 (N.D. Cal. June 28, 2018) 11

Cobra Pipeline Co. v. Gas Nat., Inc.,
132 F. Supp. 3d 945 (N.D. Ohio 2015) 8, 9

Consumer Union of U.S., Inc. v. Fisher Develop., Inc.,
208 Cal. App. 3d 1433 (Cal. Ct. App. 1989) 3

Courtesy Temporary Serv., Inc. v. Camacho,
222 Cal. App. 3d 1278 (Cal. Ct. App. 1990) 3

Cousineau v. Microsoft Corp.,
992 F. Supp. 2d 1116 (W.D. Wash. 2012) 18

Craft v. Cty. of San Bernardino,
468 F. Supp. 2d 1172 (C.D. Cal. 2006) 16

Davidson v. Kimberly-Clark Corp.,
889 F.3d 956 (9th Cir. 2018) 4, 5

Davis v. Farmers Ins. Exchange,
245 Cal. App. 4th 1302 (Cal. Ct. App. 2016) 4

Facebook, Inc. v. ConnectU LLC,
489 F. Supp. 2d 1087 (N.D. Cal. 2007) 12

Fogelstrom v. Lamps Plus, Inc.,
195 Cal. App. 4th 986 (Cal. Ct. App. 2011) 15, 18

Gonzales v. Uber Techs., Inc.,
2017 WL 8894619 (N.D. Cal. June 19, 2017) 17

Gonzales v. Uber Techs., Inc.,
305 F. Supp. 3d 1078 (N.D. Cal. 2018) ..... *passim*

Hernandez v. Stabach,
145 Cal. App. 3d 309 (Cal. Ct. App. 1983) 3

Herr v. Nestlé U.S.A., Inc.,
109 Cal. App. 4th 779 (Cal. Ct. App. 2003) 3

Hewlett v. Squaw Valley Ski Corp.,
54 Cal. App. 4th 499 (Cal. Ct. App. 1997) 3

Hill v. Nat'l Collegiate Athletic Ass'n,
7 Cal.4th 1 (Cal. 1994) ..... *passim*

In re Application for an Order Authorizing The Extension and Use of a Pen Register Device,
No. 07-SW-034 GGH, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007) 10

In re Carrier IQ, Inc.,
78 F. Supp. 3d 1051 (N.D. Cal. 2015) 13

In re Google Android Consumer Privacy Litig.,
2013 WL 1283236 (N.D. Cal. Mar. 23, 2013) 14

In re Tobacco II Cases,
46 Cal.4th 298 (Cal. 2009) 3

In re Yahoo Mail Litig.,
7 F. Supp. 3d 1016 (N.D. Cal. 2014) 15, 16

Korea Supply Co. v. Lockheed Martin Corp.,
29 Cal. 4th 1134 (Cal. 2003) 6

Law Offices of Mathew Higbee v. Expungement Assistance Servs.,
214 Cal. App. 4th 544, 561 (Cal. Ct. App. 2013) 7

Loder v. City of Glendale,
14 Cal. 4th 846 (Cal. 1997) 15

Los Angeles v. Lyons,
461 U.S. 95 (1983) 5

McGill v. Citibank, N.A.,
2 Cal. 5th 945 (Cal. 2017) 3, 5

Mintz v. Mark Bartelstein & Assocs. Inc.,
906 F. Supp. 2d 1017 (C.D. Cal. 2012) 13, 18, 20

Monsanto Co. v. Geertson Seed Farms,
561 U.S. 139 (2010) 4

Cohen v. Casper Sleep Inc.,
No. 17CV9325, 2018 WL 3392877 (S.D.N.Y. July 12, 2018) 17

Noel v. Hall,
525 Fed. App'x 633 (9th Cir. 2013) 9

Noel v. Hall,
568 F.3d 743 (9th Cir. 2009) 9

NovelPoster v. Javitch Canfield Grp.,
140 F. Supp. 3d 954 (N.D. Cal. 2014) 14

Oracle USA, Inc. v. Rimini St., Inc.,
191 F. Supp. 3d 1134 (D. Nev. 2016) 13, 14

*Palmieri v. Unite*d *States*,
No. 16-5347, 2018 WL 3542634, at *1 (D.C. Cir. July 24, 2018) 17

Presley v. United States,
No. 17-10182, 2018 WL 3454487 (11th Cir. July 18, 2018) 17

Satamodo, LLC v. Whenever Comm'cns, LLC,
No. 17-cv-0192, 2017 WL 1365839 (S.D. Cal. Apr. 14, 2017) 12

Scottsdale Ins. Co. v. Cook,
No. CV-10-1661-PHX-FJM, 2010 U.S. Dist. LEXIS 124932 (D. Ariz. Nov. 23, 2010) 4

Skinner v. Ry. Labor Executives' Ass'n,
489 U.S. 602 (1989) 16

Smith v. Maryland,
443 U.S. 735 (1979) 16

Synopsys, Inc. v. ATopTech, Inc.,
No. 13-cv-02965, 2013 WL 5770542 (N.D. Cal. Oct. 24, 2013) 12

Theofel v. Farley-Jones,
359 F.3d 1066 (9th Cir. 2004) 7, 8, 9

Trujillo v. City of Ontario,
428 F. Supp. 2d 1094 (C.D. Cal. 2006) 16, 19, 20

United States v. Miller,
425 U.S. 435 (1976) 16

Yee v. Lin,
No. C 12-02474, 2012 WL 4343778 (N.D. Cal. Sept. 20, 2012) 11

Statutes

18 U.S.C. § 2510(17) 7

18 U.S.C. § 2701(a) 7

Cal. Bus. & Prof. Code § 17203 ..... 4, 6

Cal. Penal Code § 502(e)(1)..... 10, 13

Cal. Penal Code §§ 502(c)(1), (2), (7) 12

INTRODUCTION

Two months ago, in a ruling that could just as well be describing the facts in this case, the United States Supreme Court held that a person has a reasonable expectation of privacy in the "whole of his physical movements." *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018). Like the cell-site records in *Carpenter*, Uber's surveillance in the present matter—conducted covertly through its Hell Spyware—tracked Plaintiff and Class members' locations over time, and wholly without their consent or knowledge. If anything, Uber's intrusion was *more* severe than the one in *Carpenter*. The cell-site location information in *Carpenter* provided only a blurred snapshot of the subject's movements, as the collected data could only approximate a suspect's location within a half-mile to two-mile radius. By contrast, the Hell Spyware provided Uber with a photorealistic mosaic. Uber's Hell Spyware is enough to make even Big Brother blush. It made no difference if the target of Uber's surveillance was driving down a busy street, watching TV at home, or picking up her children from school. As long as the Lyft app was running on the target's phone, Uber knew exactly where she was. Further, Uber's surveillance program was active for years, and resulted in the collection of vast amounts the deeply personal private information that Uber could (and still can) analyze and dissect on a whim absent an injunction from this Court.

Uber offers only one justification for its actions: you took the risk that we would do this by going to work for our competitor. Yet what Uber fails to understand is that *Carpenter* means what it says—people have an expectation of privacy in the whole of their movements. That people often decide to license or share their private information in order to use a smartphone or earn a living does not eliminate their right to be free from unwanted, constant surveillance, by third parties like Uber. This is exactly the line in the sand drawn by *Carpenter*: "[given] [t]he deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id*. at 2223. As California's right to privacy is broader than the right afforded by the Fourth Amendment, Plaintiff's state law privacy claim must proceed along with his statutory claims under the UCL, SCA, and CDAFA.

ARGUMENT

Plaintiff's Second Amended Complaint [D.E. 58] (July 18, 2018) (hereinafter "SAC") largely mirrors its prior iterations[1] but with several key distinctions. First, pursuant to the Court's Order re Motion to Dismiss First Amended Complaint [D.E. 51] (Apr. 18, 2018) and the Court's Order re Motion for Reconsideration [D.E. 57] (June 21, 2018), Plaintiff has amended his allegations regarding claims under the Unfair Competition Law consistent with the statutory standing requirements for injunctive relief and restitution. Second, Plaintiff has amended his allegations under the Stored Communications Act (the "SCA") by elaborating on the plausible backup purposes for which Lyft stored the unlawfully accessed communications at issue in this case. Third, Plaintiff has added additional factual allegations to support his claims under the California Computer Data Access and Fraud Act (the "CDAFA"). Finally, Plaintiff has brought his constitutional invasion of privacy claim within the context of the new law created by the Supreme Court in the intervening months in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), which has unequivocally recognized the serious invasion of privacy associated with unfettered tracking of individuals. Defendants' Motion to Dismiss [D.E. 59] (Aug. 1, 2018) (the "Motion or "Mot.") challenge these amendments as insignificant and unavailing, but Defendants are wrong. Plaintiff discusses each in turn.

I. Plaintiff Asserts Valid Claims for Violations of the Unfair Competition Law.

Plaintiff has standing under the UCL for several independent reasons. First, Plaintiff contends that as long as the Defendants still have Plaintiff's ill-gotten personal data, Plaintiff is perpetually harmed. Second, there are no assurances by the Defendants that its previous illegal actions and unfair business practices will not be reinitiated at some later point, and the surreptitious nature of its conduct makes it impossible for Plaintiff and the Class to otherwise discover any re-deployment of its spyware. Third, Defendants' unfair business practices resulted in its acquisition of Plaintiff's business assets (customers) unfairly. Finally, Defendants' conduct also caused Plaintiff to expend time and fuel for which he was never compensated. These injuries can be remedied by the UCL in the form of

[1] Plaintiff hereby incorporates by reference the extensive background information provided in its Opposition to Defendants' Motion to Dismiss Plaintiff's Amended Class Action Complaint [D.E. 41] (Nov. 22, 2017).

injunctive relief and restitution, conferring standing to pursue the same and curing the Court's noted defects in prior pleadings.

A. Plaintiff has Stated a Claim for Injunctive Relief

Defendants' illegal business practices continually harm Plaintiff; therefore, injunctive relief is proper. *In re Tobacco II Cases*, 46 Cal.4th 298, 319 (Cal. 2009) ("[T]he primary form of relief available under the UCL to protect consumers from unfair business practices is an injunction"). "Unfair Competition" is not limited to competitive conduct, it is given the "broadest possible definition." *Consumer Union of U.S., Inc. v. Fisher Develop., Inc.*, 208 Cal. App. 3d 1433, 1438 (Cal. Ct. App. 1989) (housing tract developer restricted sales to persons over age 55, in violation of Unruh Act forbidding discrimination in housing); *see also Hernandez v. Stabach*, 145 Cal. App. 3d 309, 314 (Cal. Ct. App. 1983) (slumlord used "overcrowding" as excuse for evicting who complained to authorities regarding the condition of the premises); *Courtesy Temporary Serv., Inc. v. Camacho*, 222 Cal. App. 3d 1278, 1290 (Cal. Ct. App. 1990); *Hewlett v. Squaw Valley Ski Corp.*, 54 Cal. App. 4th 499, 520 (Cal. Ct. App. 1997); *Barquis v. Merchants Collection Ass'n of Oakland, Inc.*, 7 Cal.3d 94, 111 (Cal. 1972) ("unfair competition" includes any business practice forbidden by law). Sections 17204 and 17535 permit injunctions to be sought by "any person acting for the interests of itself, its members, or the general public." *See Herr v. Nestlé U.S.A., Inc.*, 109 Cal. App. 4th 779, 789 (Cal. Ct. App. 2003) (injunctive relief under the UCL is an appropriate remedy where a business has engaged in an unlawful practice of discriminating against older workers). Injunctive relief may be sought to benefit the plaintiff, but may also be sought to benefit the general public as well. *McGill v. Citibank, N.A.*, 2 Cal. 5th 945, 955 (Cal. 2017)[2] ("public injunctive relief- i.e., relief that 'by and large' benefits the general public") (quoting *Broughton v. Cigna Healthplans*, 21 Cal.4th 1066, 1080 (Cal. 1999)).

Injunctive relief for the general public "'generally benefit[s]' the public 'directly by the elimination of deceptive practices' and 'will … not benefit' the plaintiff 'directly,' because the plaintiff has 'already been injured, allegedly, by such practices and [is] aware of them.'" *McGill*, 2

[2] Further, *McGill*, 2 Cal. 5th at 959, addressed the question whether Proposition 64 eliminated the ability of private plaintiff to seek public injunctive relief under the UCL. The court concluded that "these provisions do not preclude a private individual who has "suffered injury in fact and has lost money or property as a result of" a violation of the UCL…and who therefore has standing to file a private action-from requesting public injunctive relief in connection with that action." *Id.*

Cal. 5th at 955 (quoting *Broughton, supra*, 21 Cal.4th at 1080, n.5). Further 1992 Amendments to the UCL extended the scope of liability to past acts:

> Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments, including the appointment of a receiver, as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which have been acquired by means of such unfair competition.

Cal. Bus. & Prof. Code § 17203.

A plaintiff's standing to seek injunctive relief under the UCL requires a threat that the allegedly wrongful conduct will continue. *See Davis v. Farmers Ins. Exchange*, 245 Cal. App. 4th 1302, 1326-1327 (Cal. Ct. App. 2016) (injunctive relief improper where injuries plaintiff allegedly suffered were all in the past); *see also Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 967 (9th Cir. 2018) ("[a] plaintiff bears the burden of demonstrating that her injury-in-fact is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling") (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 143 (2010)).

Here, the collection of geolocation data (similar to a trade secret), includes personal private details that have been illegally harvested (and not destroyed) by the Defendants. This is a particularized, concrete and an actual harm to the Plaintiffs. SAC ¶¶ 10-11, 100-101. Plaintiff's allegations make clear that the sensitive geolocation data ("SGD") at issue in this case is more than his current movements to various locations, it includes historic data that invades Plaintiff's personal life. SAC ¶ 101; *see also Carpenter*, 138 S. Ct. at 2210 ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations"). Accessing Plaintiff's SGD can also provide Defendants with customer location data as well as Plaintiff's and Lyft's financial data.[3] This data is a protectable trade secret. *See Scottsdale Ins. Co. v. Cook*, No. CV-10-1661-PHX-FJM, 2010 U.S. Dist. LEXIS 124932, at *7 (D. Ariz. Nov. 23, 2010). Defendants have allegedly accessed this information but have not provided any assurances that they have destroyed the

[3] *See* SAC ¶ 58. Using the "[d]river's location information and distance travelled is necessary for calculating charges and insurance for Lyft Rides."

data concerning the personal and private movements of Plaintiff and the Class such that without injunctive relief, there is no way to know whether it will be used or disseminated in the future. SAC ¶ 152. Many putative Class members may not even be aware their information was gathered and have no way to tell if the system is implemented again in the future. Accordingly, Plaintiff continues to be harmed by the Defendants' conduct, and is entitled to injunctive relief.

Additionally, Defendants argue that it is not enough to allege that he "may work for Lyft in the future" which is contrary to law and contradicts the pleadings. (*See* Mot. at 7). As explained above, Plaintiff and the Class continue to be harmed by Defendants' retention of their data and injunctive relief can be appropriate to primarily benefit the general public. *See McGill*, 2 Cal.5th at 955 ("[t]o summarize, public injunctive relief under the UCL…is relief that has the primary purpose and effect of prohibiting unlawful acts that threaten future injury to the general public") (quotation omitted). The cases that Defendants cite to in support of their proposition that there is no harm to the Plaintiff even if he may drive for Lyft again are misguided.

Plaintiff already has standing to seek injunctive relief because he has no assurances that his data has not been destroyed, and the requirement under *Davidson* is met as he is unable to rely on the Defendants' representations that the practice has ceased. *See Davidson*, 889 F.3d at 971 (plaintiff "faces the similar injury of being unable to rely on [defendants'] representations of its product in deciding whether or not she should purchase the product in the future") (*citing Los Angeles v. Lyons*, 461 U.S. 95 (1983)). Further, if the Defendants are free to continue or to start their unfair business practice again, a practice that they conducted for almost two years,[4] Plaintiff is thereby prohibited from driving for Lyft again for fear of the same unfair business practice. Such past conduct constitutes "evidence bearing on whether there is a real and immediate threat of repeated injury." *Davidson*, 889 F.3d at 967 (quoting *Lyons*, 461 U.S. at 102) (holding there was standing to enjoin the defendant from false labeling practices because even though the plaintiff knows that the labeling is false, they could similarly be harmed in the future when purchasing a product because they will not know whether or not the false labeling practices continue).

[4] *See* SAC ¶ 52, this two-year duration reflects only the publicly known time in which the Defendants conducted this activity; the Defendants may have conducted this practice over a longer period of time, or may even continue to track Lyft drivers today.

Similarly, because Plaintiff and the Class cannot be sure whether their data will be protected or that they will not continue to be tracked while driving for Lyft, they will continue to suffer, including in deciding whether or not to drive for Lyft again. Lastly, in anticipation of the Defendants' arguments (and subsequent actions), courts have found that "[t]he mere fact that a defendant refrains from unlawful conduct during the pendency of a lawsuit does not necessarily preclude the trial court from issuing injunctive relief to prevent a post[-]trial continuation of the unlawful conduct." *Aguilar v. Avis Rent A Car System, Inc.*, 21 Cal.4th 121, 133 (Cal. 1999). Any subsequent declarations or statements by the Defendants that the conduct has been discontinued (or that the data was destroyed) does not preclude this Court from ordering injunctive relief.

In conclusion, Plaintiff continues to be harmed by the Defendants' conduct and is entitled to injunctive relief. Defendants' Motion should be denied.

B. Plaintiff has Stated a Claim for Restitution

Plaintiff is entitled to restitution for losses that resulted directly from Defendant's deployment of the Hell Spyware. In *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134 (Cal. 2003), the California Supreme Court explained that plaintiffs are entitled to "money or property that defendants took directly from plaintiff" and "money or property in which [plaintiff] has a vested interest." *Id.* at 39-40. See also, Cal. Bus. & Prof. Code § 17203 (providing that restitution is available under the statute).

Here, Defendants took, without authorization or consent, Plaintiff's geolocation data using the Hell Spyware program, and used it to depress the availability of Lyft's services to riders. As a result, Plaintiff and other Class members were forced to spend additional money (in the form of car depreciation of gas costs) and time chasing fares. Additionally, Defendants' conduct resulted in many actual customers of Plaintiff and the Class cancelling their rides due to longer wait times for Lyft drivers. SAC ¶¶ 153-155. Under either scenario, Plaintiff lost time and money for which he was not compensated. Plaintiff and the Class have an interest in their gas and time and they should be made whole again for Defendants' unfair business practices. *See* SAC ¶ 101. Defendants' contention that Plaintiff's allegations—which are original to the SAC—are immaterial is a red herring. The SAC identifies concrete, quantifiable loss suffered by Plaintiff and Class members as a direct result of

Defendants' actions. Neither the UCL's statutory language nor interpreting case law places any minimum dollar amount on the loss a plaintiff needs to suffer to attain standing. *Law Offices of Mathew Higbee v. Expungement Assistance Servs.*, 214 Cal. App. 4th 544, 561 (Cal. Ct. App. 2013) ("the quantum of lost money or property necessary to show standing is only so much as would suffice to establish injury in fact and it suffices to allege some specific, identifiable trifle of injury.") (internal citations and quotations omitted). Accordingly, because of the Defendants' business practices, Plaintiff has lost money and property that should be returned to Plaintiff, and Defendants' Motion to Dismiss should be denied.

II. Plaintiff Asserts a Valid Claim for Violations of the Stored Communication Act.

"The Stored Communications Act provides a cause of action against anyone who intentionally accesses without authorization a facility through which an electronic communication service is provided... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.'" *Theofel v. Farley-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (citation omitted). Plaintiff contends that Defendants violated the SCA by accessing Lyft's servers and obtaining the communications stored in them. SAC ¶ 130. The amended allegations now clarify that the data stored with Lyft was in electronic storage for "backup" purposes, and reaffirm that Lyft is an "electronic communication service" provider, therefore, the Plaintiff has plead facts sufficient to state a claim under the SCA. SAC ¶¶ 128-136.

A. Plaintiff has Alleged That the Data Defendants' Accessed Were Stored for Purposes of Backup Protection

Plaintiff's and the Class' communication to Lyft provides Lyft with their location, their availability to take fares, and their particular product/service that they would like to provide. This is stored with Lyft servers and is ultimately provided to authorized bona fide riders. To be in violation of the SCA, a party must "intentionally accesses without authorization a facility through which an electronic communication services is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage…" 18 U.S.C. § 2701(a). Plaintiff and the Class allege that Defendants intentionally exceeded their authorization to access Lyft's database to obtain

electronic communication while it is in electronic storage. SAC ¶¶ 56, 59, 128-136. Electronic storage is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). The Ninth Circuit takes a broad view on what constitutes "electronic storage" for backup purposes. *Theofel*, 359 F.3d 1066 (finding one purpose of emails stored on an ISP's server after delivery was to provide a second copy of the message in the event the user needs to download it again… "this functions as a 'backup' for the user.").

Defendants' claim that the data accessed was not "backed up" is not congruent with allegations in the SAC or 9th Circuit precedent. *See* SAC ¶¶ 58, 110, 133-134 ("Upon information and belief, Lyft's computer communication servers store the location of every Lyft drier, whether on duty or off duty, every few seconds"). On the contrary, Plaintiff alleges that the Lyft servers constantly take Plaintiff's location data and backs up their location every few seconds for the purposes of access of the data for fare calculation, government subpoenas, insurance purposes, and other uses. SAC ¶¶ 58, 133-134. Further, Plaintiff plausibly alleges that the data that the Plaintiff provides to Lyft are immediately sent to Lyft riders, therefore there are at least two copies of the data. A copy sent to Lyft riders and a copy stored on Lyft servers for purposes listed previously. Plaintiff is in constant communication with Lyft, with the sole purpose to connect the Lyft driver with Lyft riders. The information that is sent by Plaintiff to Lyft includes but is not limited to, their availability to take fares, the type of service product that they are willing to provide, and the cost of transportation. SAC ¶ 11. That information is stored on Lyft servers for back up purposes related to insurance inquiries, driver review, or valid subpoenas or other government requests. SAC ¶¶ 58, 133-134. Here, Defendants accessed the Lyft servers and exceeded their authorization to access that facility, as they were no longer accessing the Lyft servers to obtain Lyft services; instead they accessed the servers to track, identify, and locate Lyft drivers and Lyft riders. Plaintiff has alleged this information was plausibly stored for purposes of backup protection on Lyft's servers, and accessed in violation of the SCA.

Defendants' reliance on *Cobra Pipeline Co. v. Gas Nat., Inc.*, 132 F. Supp. 3d 945, 948, 952 (N.D. Ohio 2015) is inappropriate as it has no substantive relevance or precedential value. Defendants

contend that *Cobra Pipeline* dictates that even if the data was backed-up, the data that was accessed was not a "back-up." However, the court acknowledged the split of authority in how broad "back-up may be defined in the SCA and noted that *Theofel* takes a broader approach than courts in its circuit. Moreover, the facts of *Cobra* are distinguishable, as rather than accessing live data from a website, Plaintiff here alleges the accessed communications were continuously stored in a server every few seconds. SAC ¶ 110. It is intuitive that the data stored every few seconds is primarily stored for back-up purposes.[5] The Court here should follow the broad definition of "backup" as articulated by *Theofel*, 359 F.3d 1066 (finding access to plaintiff's emails by the defendant through an unlawful subpoena constituted a violation of the SCA).

Defendants' reliance on *Noel v. Hall*, 525 Fed. App'x 633 (9th Cir. 2013) is equally unavailing. *Noel* is factually distinguishable from this case and concerned illegally recorded communications made by the plaintiff, recording the defendant without consent.[6] The court dismissed the claim on the basis that the plaintiff, a person, was not an "electronic communication service" provider, or stored the communications at issue "pursuant to provision of such service." *Id.* at 634. Moreover, underlying the court's dismissal of the case was a distinct desire to end what it considered frivolous and vexatious litigation: "[t]hus the saga of Red the Horse survived once more and once more the federal courts became enmeshed in the petty feud between Noel and the others." *Noel v. Hall*, 568 F.3d 743, 746 (9th Cir. 2009). Indeed, the opinion Defendants relied on suggested the recording at issue in *Noel* was used for illegal purposes, and the plaintiff's "own affidavit state[d] that he stored these communications for his own use—not as part of any 'backup protection' incident to providing communications service." *Noel v. Hall*, 525 F. App'x 633, 634 (9th Cir. 2003). Therefore, both of the cases that the Defendants cite to for the proposition that the data accessed were not backups are inapplicable and unpersuasive. Instead, this Court should continue to adhere to the broad definition of "backup" delineated by the 9th Circuit in *Theofel v. Farey-Jones.*

[5] Defendants provide no authority for their statement that the "common understanding of 'backup protection[s]'-saving a second copy in case data is inadvertently deleted." Mot. at 9, n.3.

[6] In a separate lawsuit, the defendant alleged that the plaintiff violated both federal and state wiretap laws and won a judgment of $2,500 plus costs and attorneys' fees. *See Noel v. Hall*, 568 F.3d 743, 746 (9th Cir. 2009).

B. Plaintiff has Adequately Alleged Lyft's Servers Qualify as "a facility through which an electronic communication services is provided"

This Court has already considered and rejected Defendants' attempt to dismiss Plaintiff's SCA claim on the basis that Lyft is not an electronic communication service (Mot. at 10):

> Uber's lament that Plaintiff has not shown that Lyft's servers qualify as a "facility" under the Stored Communications Act reverses the burden of proof. On Uber's motion to dismiss it is its burden to show that the servers cannot possibly qualify as a "facility." It has not met that burden.

Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078, 1088 (N.D. Cal. 2018). Plaintiff continues to allege that Lyft is a facility, engaged in the operation of a technological ride-share platform facilitating communications between drivers and riders. SAC ¶¶ 3, 136. It is overtly distinguishable from the exemplar non-communication service providers proffered by Defendants: an airline, an online marketplace, a community college, and essentially an online directory. (Mot. at 10-11). Accordingly, Defendants have again failed to meet their burden at this stage of the litigation.

To the extent this Court considers Defendants' footnoted argument that the SCA claim also fails because the SCA excludes communications from tracking devices in its definition of an "electronic" communication (Mot. at 11, n. 4), Plaintiff disagrees that the Lyft driver application on a cell phone constitutes a "tracking device" and this District has never held as such. *See, e.g., Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1042-43 (N.D. Cal. 2014) (finding plaintiff stated a claim under the Wiretap Act for interception of iMessages on iPhones); *see also, In re Application for an Order Authorizing The Extension and Use of a Pen Register Device*, No. 07-SW-034 GGH, 2007 WL 397129, at *2 (E.D. Cal. Feb. 1, 2007) (commenting that "it would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices").

III. Plaintiff Asserts a Valid Claim for Violations of the CDAFA.

This Court previously dismissed Plaintiff's CDAFA claim due to "boilerplate allegations" that were impermissible under Rule 8, and because Plaintiff did not allege that he owned the data or the systems from which the data was unlawfully accessed. *Gonzales*, 305 F. Supp. 3d at 1090. Plaintiff's amendments have cured these deficiencies and Defendant's motion should be denied.

A. Plaintiff Owns the Data at Issue

The CDAFA provides that "the owner or lessee of the computer, computer system, computer

network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief." *Gonzales*, 305 F. Supp. 3d at 1090 (quoting Cal. Penal Code § 502(e)(1)). Defendants cite no cases that assert that accessing another's computer system or servers storing a plaintiff's data cannot give rise to a cause of action under § 502(c)(7) or any other provisions of the CDAFA. *See Cline v. Reetz-Laiolo*, Nos. 3:17-cv-06866, 3:17-cv-06867, 2018 WL 3159248, at *33-34 (N.D. Cal. June 28, 2018) (declining to dismiss a similar claim for the federal counterpart of the CDAFA where plaintiffs based their claims on remote access of a computer they did not own). To the contrary, Defendants cite *Yee v. Lin*, No. C 12-02474, 2012 WL 4343778, at *3 (N.D. Cal. Sept. 20, 2012), where the Court found a sufficient ownership interest in "data contained in [plaintiff's] email accounts" on servers that were owned by Yahoo and Google. Here, Plaintiff has alleged that he is the owner of a smartphone and the data transmitted to and stored in Lyft's servers that Defendants surreptitiously accessed. *See*, SAC ¶¶ 5, 54, 135, 143. At this stage of the litigation, the allegations, taken as true, are sufficient to state a claim.

Defendants attempt to use the definition of "contents" from the federal Wiretap Act to refute Plaintiff's claim of ownership over the information at issue, but that is a red herring (Mot. at 12). Defendants analogize that, if geolocation information is not "content," as defined under the Wiretap Act, "that plus common sense, shows that Plaintiff is not the 'owner' of the data for CDAFA purposes." (Mot. at 13). This is illogical. Ownership may be had over automatically generated geolocation data just as it may be had over emails, photos, and computer programs, *inter alia*, and conflating the definitions and elements of the federal Wiretap Act with the CDAFA cannot change this common sense fact. *Yee v. Lin* is not persuasive on this point. 2012 WL 4343778, at *3. In *Yee*, the Court accepted plaintiff's claim that he owned "the data contained in his email accounts." *Id.* The Court did not specify whether it was referring to emails, the text comprising the emails, data related to the emails, or the like. It was enough for the Court that Plaintiff alleged he owned data in the accessed accounts and there is no further analysis of what satisfies "ownership" of data under the CDAFA. Moreover, the Court's holding cannot be construed as accepting ownership over "the data contained in his email accounts" to the exclusion of other types of data a person could plausibly "own" – Judge

Alsup simply noted that the plaintiff need not "own" Yahoo's and Google's servers that stored the unlawfully accessed data, because he owned the data contained on them. *Id.* The strained reading of this single phrase offered by Defendants should be rejected.

Defendants go on to demand that Plaintiff "explain his theory of 'ownership'" beyond the Lyft Terms of Service that dictate Plaintiff's information belongs to Plaintiff and is licensed to Lyft (Mot. at 13). But that is not Plaintiff's burden at the pleading stage. Defendants concede that the Terms of Service give Plaintiff an ownership interest in the personal information transmitted to and collected by Lyft (Mot. at 13). Lyft's reservation of rights with respect to this data does not make Plaintiff any less of an owner, it just grants additional rights in that information to a third party, which is not Defendants.

Defendants then proceed to read a non-existent privacy requirement into the CDAFA (Mot. at 13), which should be rejected. *See, e.g., Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1091, n.5 (N.D. Cal. 2007) (rejecting defendant's attempt to dismiss the CDAFA claim due to voluntary disclosure of certain data: "Not only does this argument appear to discount unduly the right of Facebook users to disclose their email addresses for selective purposes, nothing in section 502(c) limits its applicability to confidential information."). As detailed further in Section IV, Plaintiff does have an expectation to privacy in the information unlawfully obtained by Defendants, but this is not an element of the CDAFA. Presumably this argument is a challenge to whether Plaintiff has suffered a cognizable injury under the CDAFA, but because Plaintiff's injury is not solely based on Defendant's invasion of his privacy but also involves concrete, tangible monetary losses (see Section I, *supra*, and Section III(C), *infra*), this basis for dismissal is without merit.

B. Defendants Accessed the Data Without Permission

As Defendants note, "[a]ll the relevant subsections require a showing that access was knowing and 'without permission.'" (Mot. at 14) (quoting Cal. Penal Code §§ 502(c)(1), (2), (7)). However, "circumventing technical barriers is not the *only* way to access a computer 'without permission.'" *Satamodo, LLC v. Whenever Comm'cns, LLC*, No. 17-cv-0192, 2017 WL 1365839, at *6 (S.D. Cal. Apr. 14, 2017) (emphasis in original); *see also Synopsys, Inc. v. ATopTech, Inc.*, No. 13-cv-02965, 2013 WL 5770542, at *11 (N.D. Cal. Oct. 24, 2013) ("The Court cannot find, as a matter of law, that

Plaintiff does not state a claim under the CDAFA solely because Plaintiff relies on the alleged breach of a license agreement instead of a technical breach."); *ConnectU LLC*, 489 F. Supp. 2d at 1091 (holding that defendant's access to a plaintiff's website by using information voluntarily supplied by authorized users was without permission and in violation of the CDAFA); *Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1031-32 (C.D. Cal. 2012) (granting summary judgment on CDAFA claim through use of a temporary password to gain access to another's email accounts). Indeed, "[h]olding that a defendant acts with 'permission' for purposes of the [CDAFA] any time it does not need to overcome 'technical or code based barriers in place to restrict or bar a user's access' leads to results which strain the plain and ordinary meaning of the term 'permission.'" *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1100 (N.D. Cal. 2015).

Here, Plaintiff alleges that Defendants' conduct was contrary to Lyft's Terms of Service, not contemplated by Plaintiff or Lyft, and accomplished through the use of a technical code-based program. *See, e.g.*, SAC ¶¶ 8, 54, 61, 83 134. There will be no floodgates of criminal prosecution for merely violating a website's terms of service, because that is not the only illicit conduct complained of in Plaintiff's Complaint. Just as Defendants' conduct is considered "unauthorized" under the SCA (*see Gonzales*, 305 F. Supp. 3d at 1088), it is also "without permission" under the CDAFA. The CDAFA is an "anti-hacking" statute (Mot. at 15), and Defendants' access of Lyft's servers and Plaintiff's private and confidential data is the precise conduct the statute was designed to prevent. At this stage of the litigation, Plaintiff's allegations unquestionably satisfy the "without permission" prong of the CDAFA.

C. Plaintiff Has Sustained Damages as a Result of Defendant's Conduct

Defendants misleadingly cite only a portion of the CDAFA when they state "Section 502(e)(1) refers *only* to compensatory damages for expenditure reasonably necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was not altered, damaged, or deleted by the access." (Mot. at 15) (emphasis added). However, the CDAFA permits an action for injunctive relief and compensatory damages. Cal. Penal Code § 502(e)(1). While compensatory damages "include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was not altered,

damaged, or deleted by the access," that is not the only remedy available under the statute. *See, e.g.*, *Oracle USA, Inc. v. Rimini St., Inc.*, 191 F. Supp. 3d 1134, 1146 (D. Nev. 2016) ("Defendants want to limit a plaintiff's 'compensatory damages' to only the verification and repair damages specifically mentioned by the CDAFA. In doing so they misconstrue the phrase 'shall include' as a limitation to damages under the CDAFA. Defendants' interpretation of the statute is directly contrary to the statute's plain language…'"). "[T]he plain terms of the CDAFA allows for the recovery of all compensatory damages, including economic damages." *Id.* (citation omitted).

Here, Plaintiff has alleged that as a direct result of Defendants' conduct, Plaintiff suffered monetary damages by accepting rides that were subsequently cancelled, causing lost fuel expended to seek and locate those fares for which he was not compensated, lost time, and lost economic opportunity in driving legitimate fare-paying passengers. SAC ¶ 154. Plaintiff also suffered monetary loss as a result of staunched demand for his services as a Lyft driver. SAC ¶ 155. These damages were the anticipated and desired result of Defendants' conduct. This is in contrast to the plaintiffs in *In re Google Android Consumer Privacy Litigation* where the Court dismissed plaintiffs' CDAFA claim because the damages alleged, diminished battery power, were the result of GPS tracking on the phone, not the direct result of the defendants' access of the plaintiffs' data. No. 11-MD-02264, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 23, 2013).

Ultimately, the CDAFA's "damage or loss" requirement is minimal and Plaintiff's allegations satisfy this requirement. *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 964 (N.D. Cal. 2014) ("[A]ny amount of damage or loss caused by the defendant's CDAFA violation is enough to sustain the plaintiff's claims."); *see also*, *Capitol Audio Access, Inc. v. Umemoto*, 980 F. Supp. 2d 1154, 1159-60 (E.D. Cal. 2013) (denying motion to dismiss where plaintiff alleged only that it had been injured by defendant's violations of the CDAFA, and Defendant failed to show that the claim was "implausible.").

IV. Plaintiff Asserts a Valid Claim for Constitutional Invasion of Privacy.

In determining whether the intrusion upon a privacy interest is consistent with the protections afforded by the California Constitution, courts will consider three elements: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by

defendant constituting a serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 39-40 (Cal. 1994). "These elements are not a categorical test, but rather serve as threshold components of a valid claim to be used to 'weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant.'" *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1037 (N.D. Cal. 2014) (quoting *Loder v. City of Glendale*, 14 Cal.4th 846, 893 (Cal. 1997)). Thus, unless the court concludes the alleged intrusion is *de minimis*, it must also assess defendant's justification for the intrusion. *Loder*, 14 Cal.4th at 894-95 (citing *Hill*). Only where "the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests" may the question of invasion of privacy be adjudicated as a matter of law. *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 990 (Cal. Ct. App. 2011).

A. Plaintiff Alleges Invasion of a Legally Protected Privacy Interest

Defendants base their motion to dismiss Plaintiff's claim for invasion of privacy on an impermissibly narrow interpretation of the holding in *Carpenter* and a broad interpretation this Court's prior Order. This Court previously held that Plaintiff failed to allege a (1) a reasonable expectation to privacy, or (2) a *serious* invasion of privacy. However, Plaintiff unequivocally alleged a "protected privacy interest." *Gonzales*, 305 F. Supp. 3d at 1091. Applying *U.S. v. Jones*, 565 U.S. 4001, 411 (2012), the Court held that individuals have a protected privacy interest in "home addresses and arguably precise geolocation data." Plaintiff's Complaint was not deficient in this regard and maintains allegations sufficient to state a protect privacy interest after amendment.

This Court also implied that the Supreme Court's decision in *Carpenter* would determine whether there was a protected privacy interest in historical location:

> We know location is private, because the Supreme Court even requires… probabl[e] cause for law enforcement to real time track locations, so there's no question that the location is private information… The Supreme Court is going to decide whether historical call site information requires probable cause… There really isn't any dispute, I think, that real time requires probable cause, so there's an understanding that that's private.

See, Tr. of Proceedings (Aug. 31, 2017), at 26:8-27:3 (attached to Marker Decl. as Exhibit 1, filed concurrently herewith). Now it has. *See, Carpenter*, 138 S.Ct. at 2221 (finding the government must obtain a warrant supported by probable cause before acquiring historic cell site location information).

B. Plaintiff Maintained a Reasonable Expectation of Privacy in his SGD

"A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal.4th at 37. To be considered reasonable, the plaintiff "must not have manifested by his or her conduct voluntary consent to the invasive actions of the Defendant." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1038 (citing *Hill*, 7 Cal.4th at 26). Prior to *Carpenter v. United States*, cell-site location information fell into the business records category along with information like telephone numbers dialed (*Smith v. Maryland*, 443 U.S. 735 (1979)) and bank records (*United States v. Miller*, 425 U.S. 435 (1976)). 138 S.Ct. at 2216. This type of information is exempt from warrant requirements because it is disclosed to third parties such that individuals have no reasonable expectation to privacy in it. The Supreme Court has now clarified that similarly limited disclosure does not render an expectation of privacy in more revealing information unreasonable.[7]

Protections guaranteed by the Fourth Amendment are similarly protected by Article I Section I of the California Constitution, and the analysis regarding the reasonableness of the privacy interest and the severity of the invasion are the same. *See, Trujillo*, 428 F. Supp. 2d at 1120. Accordingly, Plaintiff maintains a reasonable expectation of privacy in his historical location information. *Carpenter* stands for the proposition that the Fourth Amendment requires the government to obtain a warrant to retrieve historical cell-site location information because individuals have a legally

[7] The privacy rights guaranteed by the California Constitution are just as strong as the protections guaranteed by the Fourth Amendment to be free from unreasonable searches by the government, and in some cases, stronger. *See, e.g., Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1120 (C.D. Cal. 2006), *aff'd sub nom. Bernhard v. City of Ontario*, 270 Fed. App'x 518 (9th Cir. 2008) (*infra*); *Am. Acad. of Pediatrics v. Lungren*, 16 Cal. 4th 307, 326, (Cal. 1997) ("most significantly, not only is the state constitutional right of privacy embodied in explicit constitutional language not present in the federal Constitution, but past California cases establish that, in many contexts, the scope and application of the state constitutional right of privacy is broader and more protective of privacy than the federal constitutional right of privacy as interpreted by the federal courts.") (comparing *Hill*, 7 Cal. 4th 1, with *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989)); *Craft v. Cty. of San Bernardino*, 468 F. Supp. 2d 1172 (C.D. Cal. 2006) (granting summary judgment for plaintiffs on constitutional privacy claims on the same basis as Fourth Amendment claims). Indeed, the Fourth Amendment provided substantial foundation for drafting the privacy amendment to the California constitution. *See, Hill*, 7 Cal. 4th at 28-32 (detailing the federal privacy interests that influenced passing the California constitutional interests); *Gonzales*, 305 F. Supp. 3d at 1091.

recognized, reasonable expectation to privacy in the same. As in *Carpenter*, "this case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. "[W]hen the Government accessed CSLI from the wireless carries, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements." *Id.* at 2219. So too, here. In accessing the stored geolocation data, Defendants invaded Plaintiffs' reasonable expectation of privacy in the whole of his physical movements. "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection." *Id.* at 2223.

The cases cited by Defendant are entirely inapposite. *Presley v. United States*, No. 17-10182, 2018 WL 3454487 (11th Cir. July 18, 2018) concerned bank records which, per *Miller*, have always been considered information that individuals do not have a reasonable expectation in maintaining private, advances in technology have not changed this characteristic. This is unlike cell-site location information (which Defendants have already admitted is substantially equivalent to the information at issue in this case in successfully obtaining dismissal of claims for violations of the Wiretap Act), which is now afforded such protections under the Fourth Amendment post-*Carpenter* in light of technological advances changing the breadth of information revealed by the same.

In *Palmieri v. United States*, the Court found no reasonable expectation to privacy in information obtained when Facebook friend of individual subject to investigation used access she had been given by that subject in accepting her friend request. No. 16-5347, 2018 WL 3542634, at *6, n.7 (D.C. Cir. July 24, 2018). The Court explicitly contrasted the subject-matter of that search with that in *Carpenter*, stating plaintiff had not alleged "a detailed chronic[ling] of the individual's physical presence compiled every day, every movement, over several years." *Id.* (alteration in original).

Finally, in *Cohen v. Casper Sleep, Inc.*, the Court actually cited *Carpenter* in support of plaintiff's "well-founded" desire to maintain privacy due to "seismic shifts in digital technology," but ultimately found that *New York* does not recognize a claim for general invasion of privacy under General Business Law 349. No. 17CV9325, 2018 WL 3392877, *4, *8 (S.D.N.Y. July 12, 2018)

("Cohen's allegations are unsettling … '[w]ith just the click of a button, [Defendants] can access each [visitor's] deep repository of … information at practically no expense.'") (*quoting Carpente*r, alterations in original).

The third-party exception relative to Fourth Amendment privacy rights (*Gonzales'* limited consent to Lyft for business purposes) is no different than the consent given by the Defendant in *Carpenter* to his cell phone service provider. *See, e.g.*, Def.s' Mot. Dismiss, No. 3:17-cv-02264-JSC, 2017 WL 8894619 (June 19, 2017) (citing *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1127 (W.D. Wash. 2012) ("A close look at the nature of CSLI reveals that it is extremely similar to the information that was allegedly transferred to Microsoft. One court described CSLI as the cell phone's unique identification number which is transmitted to cell towers, and which can 'with a fair degree of precision' approximate the location of the phone based on the location of the towers.")).

The data collected by Defendants was password protected, limitedly available by registered users of Lyft, and used by Lyft under limited Terms of Service. Plaintiff never gave permission to competitors to access this data, and even those with the limited access described above could not have tracked Plaintiff on a daily basis or amassed the data gathered by Defendants. As with CSLI, Plaintiff alleges that "the information collected with a potentially infinite amount of historical waypoints that Uber intercepted and amassed in real time over several years painting a vivid, intimate, portrait of one's life including, but not limited to, 'home' and 'work' locations, identity, employment hours, work schedule, and employment history." SAC ¶ 116. Accordingly, there is a reasonable expectation of privacy to geolocation data at issue in this case and it was not vitiated by the limited consent given to Lyft and potential riders to facilitate specifically enumerated ride-share goals. *See, e.g.*, *Mintz*, 906 F. Supp. 2d at 1033 (C.D. Cal. 2012) (finding reasonable expectation of privacy in password protected emails).

C. Defendants' Conduct Amounts to a Serious Invasion of Plaintiff's Privacy Interests

Previously, this Court held that the violation alleged by Plaintiff could not be considered "serious" in a manner sufficient to maintain a cause of action for violation of his constitutional rights, comparing the facts to *Fogelstrom*. *Gonzale*s, 305 F. Supp. 3d at 1092-93. In *Fogelstrom*, plaintiff alleged that defendant, a lamp store, routinely requested its customers provide their zip codes during

credit card transactions, which it then sent to a third-party credit reporting agency to obtain mailing addresses for marketing purposes. 195 Cal. App. 4th at 989. The court found that cases recognizing "residential" privacy interest were too distinguishable from the facts at hand, and even if recognized in this case, mailing coupons and other advertisements was not "an egregious breach of social norms, but routine commercial behavior." *Id.* at 992.

In light of *Carpenter*, however, it is clear that surreptitious conduct by Defendants was not simply "routine commercial behavior" but an egregious breach of social norms. If similar conduct by the government requires probable cause and a warrant, society is not prepared to accept such conduct as merely "routine" from private actors. "As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Carpenter,* 138 S.Ct. at 2217 (quotation omitted). The "unblinking" technology deployed by Defendants is akin to the silent video recording of employees in their locker room complained of in *Trujillo* and found to be in violation of the state and federal constitutional guarantees and is unmitigated. 428 F. Supp. 2d at 1107 ("that the video surveillance here could have been conducted in a more intrusive manner, recording the officers in the showers, having an audio component, or having a roving camera, in no way diminishes the severity of the search."). The collection of this information by Defendants was a serious invasion of Plaintiff's privacy, regardless of "what Uber did, if anything, with this information." *Gonzales*¸ 305 F. Supp. 3d at 1092. As alleged in the Complaint, however, Defendants used this information at a minimum to obtain a competitive advantage over Lyft and harm Plaintiff's ability to secure and complete rides and earn income from the same.

D. Defendants Have No Legitimate Justification for their Invasion

"The diverse and somewhat amorphous character of the privacy right necessarily requires that privacy interests be specifically identified and carefully compared with competing or countervailing privacy and nonprivacy interests in a 'balancing test.'" *Hill*, 7 Cal. 4th at 37. Put differently, only when a legitimate competing interest outweighs a more than *de minimis* invasion of privacy can a court permit such conduct. *Id*. at 38. Viewed as a whole and in light of the Supreme Court's recent acknowledgment of the gravity of intrusions of this nature, the Court should consider Defendants'

invasion to surpass the *de minimis* standard necessitating analysis of the justification for the invasion. In this case, there is no justifiable competing interest such that "the balance therefore weighs decisively in favor of Plaintiff." *Mintz,* 906 F. Supp. 2d at 1034.

Even if this Court were to consider commercial competition to be a legitimate interest to compete with Plaintiff's expectation of privacy, the myriad alternatives to achieving Defendant's goals undermines any potential justification. *See*, *Trujillo*, 428 F. Supp. 2d at 1121 (finding plaintiffs had rebutted any countervailing interest defense because they presented evidence that other feasible and effective alternatives to surveillance existed).

This Court, in this case, relied on Fourth Amendment jurisprudence in determining what rights are protected, and should continue to do so in determining what expectations of privacy are reasonable under the circumstances. Defendants' conduct was a serious invasion of a legally protected privacy interest, perpetrated solely to undermine Lyft's competitiveness and harm Lyft drivers like Plaintiff and the Class. For these reasons, Defendants' motion to dismiss Plaintiff's claim for constitutional invasion of privacy must be denied.

CONCLUSION

Based on the foregoing, Plaintiff respectfully requests this Court DENY Defendants' motion.

Respectfully submitted,

Dated: August 15, 2018

ZIMMERMAN REED LLP
/s/ Caleb Marker
Caleb Marker
E-Mail: Caleb.Marker@zimmreed.com
2381 Rosecrans Ave., Suite 328
Manhattan Beach, CA 90245
(562) 216-7380 Telephone

Mark Burton
E-Mail: mburton@audetlaw.com
Michael McShane
E-Mail: mmcshane@audetlaw.com
Ling Y. Kuang
E-Mail: lkuang@audetlaw.com
AUDET & PARTNERS, LLP
711 Van Ness Ave., Suite 500
San Francisco, CA 94102
(415) 568-2555 Telephone

Counsel for Plaintiff and the Class